サイバー空間における犯罪捜査とプライバシー

堀田周吾

一　サイバー犯罪への手続法的対応の現在地
　1　「サイバー犯罪」の問題
　2　本稿の目的
二　サイバー空間と合衆国憲法修正四条
　1　修正四条の「捜索」の意義
　2　通信に関するプライバシーの保護
　3　近時の議論状況
三　結びにかえて

一　サイバー犯罪への手続法的対応の現在地

1　「サイバー犯罪」の問題

インターネットの利用者数は年々増加を続けており、平成二五年には一億人を超え、人口普及率も八〇％を上回った[1]。インターネットがもはや社会の欠くべからざるインフラストラクチャーの一つであることは疑いない。他方、情報通信ネットワークの発展による負の産物として、サイバー犯罪の増加がある。平成二五年中の検挙件数は過去最多を記録しており[2]、サイバー犯罪への対応は、喫緊の課題の一つである。

ところで、この「サイバー犯罪」という呼称自体、刑事法が直面している問題の難しさを端的に表しているように思われる。

電子計算機（コンピュータ）に関わる犯罪は、かつて「コンピュータ犯罪」と呼ばれたが、そこで想定されたのは、従来から処罰の対象とされてきた行為をコンピュータに向けて、あるいはコンピュータを悪用して実行する事犯であった[3]。刑法は、昭和六二年の改正で、電磁的記録にかかる偽造・毀棄関連行為と電子計算機にかかる業務妨害・詐欺関連行為を処罰する規定を新設するほか、財産的情報の不正取得に関しては、情報が化体された有体物を客体とする窃盗罪、横領罪の成立を認める等の解釈による対応をしてきた[4]。平成一三年の刑法改正で創設された支払用カード電磁的記録に関する罪、とりわけ一六三条の四の支払用カード電磁的記録不正作出準備罪は、情報の不正取得行為の処罰に向けられたものであるとみることもできよう[5]。

コンピュータ犯罪に対する刑事訴訟法（とりわけ捜査分野）の対応は、電磁的記録を証拠として取り扱うところから出発する(6)。有体性のある証拠を念頭に置いた刑事訴訟法において、捜索・差押えの対象は電磁的記録自体ではない。電磁的記録が記録・保存された媒体（電磁的記録物）を証拠として捜索し差し押さえるにあたり、可視性・可読性を欠くという電磁的記録の特殊性を現行法に適合させることが求められた(7)。

この種の事犯が主に「コンピュータ犯罪」と呼ばれた時代、刑法・刑事訴訟法の課題は、「現実世界（real world）」で行われる犯罪現象に対応する体系・理論に「コンピュータ」をいかに組み込むか、ということであったといえよう(8)。しかし、その後、情報通信ネットワークの発展は、「現実世界」とは別の「サイバー空間（cyberspace）」を作り出し、情報セキュリティを脅かす新たな犯罪が出現した。平成一一年の不正アクセス禁止法は、状況の変化にいち早く対応したものであった。「ハイテク犯罪」「ネットワーク犯罪」といった呼称が多く用いられるようになったのも、この頃からである。

「サイバー犯罪」の定義は様々である。例えば、警察白書は、「高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪」と定義した上で、不正アクセス禁止法違反、コンピュータ・電磁的記録対象犯罪等、ネットワーク利用犯罪（その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪）という三類型を挙げる(9)。第三の類型には、ネットワークを介して実行される詐欺や児童買春・児童ポルノ禁止法違反等も含まれる。また、わが国が平成二四年に批准した「サイバー犯罪に関する条約（Convention on Cybercrime）」も、「コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの秘密性、完全性及び利用可能性に対して向けられた行為並びにコンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの濫用を抑止する」ことを同条約の目的とつつ、具体的類型として

は、児童ポルノに関連する犯罪（第九条）、著作権及び関連する権利の侵害に関連する犯罪（第十条）も挙げている[10]。こうした定義は、情報通信ネットワークを犯罪の手段として利用する場合を広く含めて「サイバー犯罪」と捉えるものである。

他方で、「サイバー空間」においてのみ実行可能な犯罪類型に限定し、「コンピュータ・セキュリティ（コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データの機密性、完全性及び可用性）に関する危害を意図した反社会的侵害行為であって、コンピュータ・システム、コンピュータ・ネットワーク及びコンピュータ・データを手段として伝統的犯罪を行うものを除いたもの」とする説明も提唱されている[11]。平成二三年の刑法改正で新設された不正指令電磁的記録作成等罪（一六八条の二）および同取得罪（一六八条の三）は、まさにそこで想定されるものの一類型である。

このような狭義の「サイバー犯罪」概念が示唆するのは、「現実世界」の延長線上にあった従来の「コンピュータ犯罪」とは異なる、新しい問題状況である。

2　本稿の目的

サイバー犯罪が深刻化するにつれ、捜査手続との関係では、二つの側面が特に注目される。

第一に、犯罪に関連する電磁的記録を被疑者および関係者とは無関係の第三者が保有するようになったことである。より具体的には、証拠としての電磁的記録をインターネット・サービス・プロバイダー（ＩＳＰ）を通じて、電子メール等の方法で送受信する際に、当該通信の内容をＩＳＰが把握しうるという状況である[12]。また、電磁的

記録が被疑者等の手元の端末ではなく、通信事業者等が提供するオンライン・ストレージに保存されている場合にも生じる。近年、いわゆるクラウド・コンピューティングの普及によって、データの保管先は個別の端末から「クラウド」へ移行しつつある。

第二に、現実世界で行われる犯罪において犯行の形跡を無くすなどの工作が行われるのと同様に、サイバー空間における犯罪の探知・追跡を困難にする高度な技術が生まれていることである[13]。これに対応するためには、サイバー空間における活動の入り口の段階、すなわちパソコン等の端末からインターネットに接続する際にＩＳＰに保存される通信履歴を捜査機関が把握できるようにしなければならない[14]。平成二三年度総合セキュリティ対策会議（座長：前田雅英教授）の報告書（『サイバー犯罪捜査における事後追跡可能性の確保に向けた対策について』）でも、次のような指摘がされている。「現実空間において、犯行現場から足跡、指紋等を分析し、犯人に到達できるように、サイバー空間で行われた犯罪についても、犯人が利用したインターネット端末や経由したサーバの記録などから得られる各種情報を分析するなどして追跡し、犯人まで到達できること、すなわち事後追跡が可能であることが必要である[15]。」

平成二三年の刑訴法改正は、これらの問題について一応の解決を見るものであった。新設された九九条の二は、捜索の対象である電子計算機と回線で接続された他の記録媒体に保存された電磁的記録をいわゆるリモート・アクセスの手段を通じて差し押さえることを可能にした。また、一九七条三項以下では、通信事業者が業務上記録している電気通信の送信元・送信先・通信日時その他の通信履歴について、一定期間これを消去しないよう保全要請することが認められた。

もっとも、通信をとりまく状況は急激に変化している。通信履歴の保全に関するわが国の新規定は、二〇〇一年

に欧州評議会が採択したサイバー犯罪条約が「通信記録の迅速な保全及び部分開示（第一七条）」として、「通信の伝達に関与したサービス・プロバイダが一であるか二以上であるかにかかわらず、通信記録の迅速な保全が可能となることを確保すること」を定めたことを受けたものである。他方、二〇一四年四月、欧州司法裁判所は、過去六ヶ月以内の全ての通信履歴を最大二年間保存することを義務づけたEUのデータ保存指令[16]を無効とする判決を下した[17]。アメリカ合衆国においても、国家安全保障局によるインターネット上の個人情報収集活動が明るみになり、インターネットにおけるプライバシー保護の議論が活発化している。「ビッグ・データ」の時代となった今日、EUとアメリカ合衆国とで状況は違えど、プライバシーに関して変革が起きつつあることは間違いないようである[18]。

サイバー空間の問題に関しては、わが国も諸外国の動向と無関係ではいられない。無論、欧州司法裁判所が右の無効判決で問題としたのは、当該EU指令が通信内容を含む全てのデータを包括的に長期間保存することを義務づけた点であるから、個別の事件に関して必要なものを特定して通信履歴のみの保全を要請するわが国の規定とは直接関連しない。しかし、国境を容易に超えることはサイバー空間（サイバー犯罪）の特性の一つであり、欧米の成り行きを注視する必要があろう。

そこで、本稿では、さしあたりアメリカ合衆国の現況を探るべく、情報通信にかかるプライバシー保護をめぐるアメリカ合衆国の判例および学説の動向を概観する。

（1）『情報通信白書（平成二六年版）』三三七頁。
（2）『警察白書（平成二六年版）』一〇六頁。
（3）西原春男「コンピュータの導入と刑事法上の諸問題」ジュリ四八四号（一九七一年）三六頁、板倉宏「コンピュータ犯罪と刑事法」ジュリ七〇七号（一九八〇年）一四四頁以下など。

（4）東京地判昭和五九年六月二八日刑月一六巻五＝六号四七六頁、札幌地判平成五年六月二八日判タ八三八号二六八頁、東京地判平成九年一二月五日判時一六三四号一五五頁、東京地判平成一〇年七月七日判時一六八三号一六〇頁など。

（5）前田雅英＝堀田周吾「個人識別情報の刑事的保護―『ＩＤ犯罪』の現状―」法律のひろば六一巻一〇号（二〇〇八年）二〇頁。

（6）各和吉四郎「コンピュータ犯罪と捜査」警論二八巻三号（一九七五年）六八頁。

（7）廣畑史朗「コンピュータ犯罪と捜索・差押え」警論四一巻三号（一九八八年）六五頁以下、安冨潔『刑事手続とコンピュータ犯罪』（二〇〇〇年）一五六頁。

（8）佐久間修「情報犯罪・サイバー犯罪」一三四八号（二〇〇〇年）一〇九頁も、「実質的にも、刑法典の枠組みを何ら変えるものでなく、旧来の諸犯罪に近接する違法行為を現行法規で捉えるための法改正であった」と指摘する。

（9）『警察白書（平成二六年版）』一〇六頁。

（10）外務省による訳文を引用。［http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf（最終訪問：二〇一五年三月二〇日）］

（11）岡田好史「サイバー刑法の概念と展望」専法一一八号（二〇一三年）七〇頁。

（12）この点は、信書を開封できない郵便局や通話内容を傍受・録音しない電話会社とは異なる。

（13）四方光「サイバー犯罪捜査における事後追跡可能性と通信の秘密」警論六六巻一二号（二〇一三年）二四頁以下。

（14）四方光・前掲注（13）四〇頁。

（15）警察庁ＨＰ［http://www.npa.go.jp/cyber/csmeeting/h23/pdf/h23.pdf（最終訪問：二〇一五年三月二〇日）］。

（16）Data Retention Directive 2006/24/EC.

（17）CJEU, C-293/12 Digital Rights Ireland and 594/12 Seitlinger and Others.

（18）宮下紘「プライバシー・イヤー二〇一二――ビッグ・データ時代におけるプライバシー・個人情報保護の国際動向と日本の課題」Ｎｅｘｔｃｏｍ一二号（二〇一二年）三二頁以下、同「ビッグデータの活用とプライバシー保護」法セミ七〇七号（二〇一三年）八頁以下を参照。

二　サイバー空間と合衆国憲法修正四条

1　修正四条の「捜索」の意義

(1) 侵入理論

合衆国憲法修正四条は、「身体、住居、文書、所有物（persons, houses, papers, and effects）について、不合理な捜索および押収（unreasonable searches and seizures）をされない人民の権利は、侵されてはならない」とする合理性条項（Reasonableness Clause）と、「いかなる令状も、誓約または確約によって裏付けられた相当な理由に基づき、かつ、捜索される場所および押収される人または物を明示するものでなければ、発付されてはならない」とする令状条項（Warrant Clause）という二つの独立した条項から構成される。当初、「不合理な捜索および押収」とは、本条が保護する領域に対して、令状なくして捜索・押収を行うことであると理解されていた(19)。

一八八六年のボイド（Boyd）判決(20)によれば、修正四条が保護の対象とするのは、政府の支配が及ばない私有財産である(21)。輸入物品を記載した私的書類等に対する裁判所の提出命令の当否が争われた事案で、合衆国最高裁は、「私的財産に対する侵害は、たとえ僅かであっても、すべて侵入（trespass）である」と述べたイギリスのエンティック（Entick）判決(22)を引用しつつ、「個人の安全、個人の自由、私有財産に関する不可侵の権利に対する侵害」が修正四条違反の核心を構成すると判示した(23)。本判決が、盗品や没収品、密封された課税対象品と、私的な帳簿

や文書とを区別し、前者にのみ政府の支配が及ぶとした[24]理由は、前者の物品に関しては、政府の利益が個人の利益に優越すると判断されたからである[25]。

ボイド判決は、修正四条による保護の対象が「身体、住居、文書、財産」の字義どおりの私有財産であるとする財産権理論（property theory）を採用した[26]。これは財産権に価値の序列を与え、個々の財産に関して政府の側に優越的利益が存在するか否かの選別を要求するものである。その表れの一つとして、「単なる証拠の原則（mere evidence rule）」がある。一九二一年のグールド（Gouled）判決[27]は、刑事手続で個人に対する証拠を確保する目的で捜索令状を用いることは許されない旨判示しており、証拠利用目的のみでは政府の優越的利益が認められないことを明らかにしたのである。

ボイド判決が修正四条に関する目的的解釈を施したとみるならば、これに対して、一九二八年のオルムステッド（Olmstead）判決[28]が行ったのは文理解釈である[29]。本件は、密造酒取引への関与が疑われた被告人の電話上の会話を傍受したという事案であり、連邦捜査官は被告人の住居等に立ち入ることなく、公共の電話線に盗聴器を取り付けたため、修正四条にいう捜索または押収に該当するか否かが争われた[30]。タフト（Taft）長官による法廷意見は、ボイド判決等で行われた解釈が憲法の起草者たちの意図に沿うものであることを認めつつ、しかし、身体・住居・文書・所有物の本来の意味を超えた拡張解釈が正当化されるものではないと述べた[31]。そして、「被告人の身体、文書、有形の私有財産に対して捜査官による捜索・押収、または押収目的でその住居や宅地に対する物理的な侵入が行われた場合」以外に修正四条違反を認めた判例は過去にないとして、本件傍受が修正四条の捜索・押収には該当しないと判示したのである[32]。

この時期の合衆国最高裁判例は、オルムステッド判決以外にも、住居・身体・文書・所有物に対する物理的な侵

入のみが修正四条の規制を受けるという判断をしている。[33]「侵入理論（trespass theory）」[34]と呼ばれるこのような考え方は、オルムステッド判決が行った文理解釈と相まって、修正四条の適用を硬直的なものとした。そのため、新しい技術の登場に伴い、合衆国最高裁が「侵入理論」を放棄することは、ある意味で必然的な流れだったといえる。[35]

（2）カッツ判決

オルムステッド判決にブランダイス裁判官による有名な反対意見が付されたことは周知のとおりだが、[36]そこで言及されたプライバシー権が合衆国最高裁の多数意見として定着するのは一九六七年のカッツ（Katz）判決[37]以降のことである。

カッツ判決に先立ち、同年のヘイデン（Hayden）判決[38]が、従来の修正四条の解釈を批判している。同判決は、「純粋な証拠物件に対する捜索によるプライバシー侵害は、犯罪供用物件・犯罪の果実・禁制品に向けられた捜索によるそれを超えるものではない」[39]として「単なる証拠の原則」を破棄し、さらに、捜索・押収にかかる政府の権限を財産権が規制するという前提に疑義が生じていること、修正四条の主たる目的が財産権ではなくプライバシーの保護にあることに言及した。[40]

これに続くカッツ判決で、ステュワート（Stewart）裁判官による法廷意見は、「修正四条は場所（places）ではなく人（people）を保護するものである」[41]という言葉とともに、「他人から独りにしておいてもらう権利（right to be let alone by other people）」[42]としてのプライバシーが修正四条による保護の対象であることを明示した。本件では、連邦捜査官が、被告人が使用した公衆電話ボックスの外側に電子盗聴録音機を取り付け、被告人の会話を令状

なしに傍受したという事案であり、前掲オルムステッド判決の法廷意見に従えば、「物理的な侵入」が認められない。しかし、本判決の法廷意見は、「人が自ら認識して公衆に対して晒した事項については、たとえその者の自宅内や職場内であっても、修正四条の保護を受けない。しかし、人が私的なものとして保持したいと考える事項については、たとえ公衆からのアクセスが可能な領域であっても、憲法上保護される[43]」と述べて、侵入理論とは一線を画する判断を示したのである。

ハーラン（Harlan）裁判官の同意意見は、プライバシーが保護されるための要件として、①主体がプライバシーに対して実際的な（主観的な）期待を表明していること、②社会がその期待を「合理的」と認めるものであることを挙げた[44]。これを受けて、以後の合衆国最高裁は、「プライバシーの合理的期待（reasonable expectation of privacy）」が認められるか否かを修正四条の適否における重要なメルクマールとしてきた。

（3）ジョーンズ判決

二〇一二年のジョーンズ（Jones）判決[45]は、「プライバシーの合理的期待」を中心に据えてきたカッツ判決以降の合衆国最高裁判例の傾向に対して、やや異質な判断を示すものである。

本件の事案は、薬物取引の嫌疑がかけられたXが運転する車両にGPS（全地球測位システム）による追跡装置を取付けたというものである。Xが経営するナイトクラブに対する見張りやカメラによる監視、Xの携帯電話の傍受などから得られた情報に基づいて、捜査機関が裁判所から取得していた令状は、コロンビア特別区（DC）内において、一〇日間に限りGPS追跡装置の取付けを許可するものであった。にもかかわらず、一一日目以降も、D

Cではなくメリーランド州内において、装置の使用は継続され、その後二八日間にわたりXの車両の位置情報が捜査機関に送信されたのである[46]。

公判において、GPS追跡装置から得られた証拠の排除をXが申し立てたところ、連邦地方裁判所は、車両がXの自宅敷地内の車庫に駐車されていた際に得られた部分を除いて、証拠能力を認めた[47]。陪審の評決不成立を経て、共謀関係にあるとされる共同被告人らとともに再び公判に付されたところ、最初の事件で認められた証拠に基づき、Xらに対して有罪の評決が下された[48]。しかし、Xらの上訴を審理したDC巡回控訴裁判所は、令状によらずして使用されたGPS追跡装置で得られた証拠を許容することは修正四条に違反するとして、Xに対して無罪判決を下したのである（控訴審判決については後述する）。

合衆国最高裁の九名の裁判官は、本件におけるGPS追跡装置の取付けと使用が修正四条の捜索にあたるという結論で一致したものの、二つの同意意見が提出された。ここでは、スカリア（Scalia）裁判官による法廷意見をまず検討する。

「本件で起きたこと――政府が、情報を収集する目的で、私有財産を物理的に占有した（occupied）ということ――を明確にすることが重要である。当裁判所は、そのような物理的侵害（physical intrusion）が修正四条の制定時から意味するところの『捜索』に該当するであろうことに疑いを持たない[49]。」

「政府は、捜査官が接触したジープの領域（車体の底面部）と、誰からも観察可能な公道におけるジープの所在について、Xに『プライバシーの合理的期待』は認められないとして、［カッツ判決におけるハーラン裁判官の基準］によれば本件では捜索が行われていない旨を主張する。しかし、修正四条にかかるXの権利は、カッツ判決の

公式（formulation）によって肯定されるものでも否定されるものでもないから、当裁判所が政府の主張を吟味する必要はない。基本的には、政府からのプライバシー保護が、修正四条の制定当時に存在していたのと同水準のものが維持されることを当裁判所は保証しなければならない。既に述べたとおり、当裁判所における歴史の大半を通じて、修正四条は、それが列挙した領域（身体、住居、文書、所有物）への政府の侵入に対する懸念を具体化したものであると理解されてきた。カッツ判決はその理解を否定したものではない。[50]」

本判決の法廷意見は、ＧＰＳ追跡装置の取付けを私有財産である車両に対する「物理的侵害」と捉えて、修正四条の「捜索」に該当すると判断した。カッツ判決はこのような伝統的な判例理論を否定したものと一般に理解されているが、他方で、スカリア裁判官は「プライバシーの合理的期待」に対する懐疑的な立場をこれまでも示してきた[51]。しかし、法廷意見は、カッツ判決以降の合衆国最高裁の立場を否定することはせず、「プライバシーの合理的期待」の基準はそのような「コモン・ロー上の侵入テスト（common-law trespassory test）」に追加されたものであり、代替するものではないと述べたのである[52]。

本件事案の処理に関して、法廷意見が車両への物理的侵害を問議した点は、ソトマイヨール裁判官もその同意意見で支持を表明している。「多数意見によって適用された侵入テストは、侵さざるべき憲法上の最低水準――政府が情報を収集する目的で私有財産を物理的に侵害した場合は、捜索に該当するということ――を示したものである。本件を判断するためにはこの原則を再確認することで足りる[53]。」

このように、ジョーンズの判決の法廷意見は、「プライバシーの合理的期待」を主軸としてきた立場とはやや異なる判断を示している。ただし、情報通信との関係では、法廷意見も、「侵入を伴わない、電子信号が単に伝達さ

れる場合については、カッツ判決の判定方法の対象であり続ける[54]」と判示しており、従来のカッツ判決の系統に属する諸判例が今なお重要な意味を持つ。この点は次節で検討する。他方、ジョーンズ判決に付された同意意見は、いわゆる「モザイク理論」への親和性を示したものと受け取られており、別途の検討を要する。この点は、次々節で扱う。

2　通信に関するプライバシーの保護

(1) 二つの「通信」

カッツ判決の「プライバシーの合理的期待」の基準は、郵便・電話・インターネット等の通信について、通信の中身とそれ以外とを区別し（content/non-content distinction）、通信の内容、目的、意味に関わる前者に手厚い保護を与える反面、送り手と受け手その他通信に関わる外形的な情報[55]を捜査機関が取得することについては規制を比較的緩やかにするという二元的扱いを確立した（以下、便宜的に「区別論」と呼ぶ[56]）。

カッツ判決以前にも同様の枠組みはみられた。政府による郵便規制の当否が争われた一八七七年のジャクソン（Jackson）ケース[57]で、合衆国最高裁は、手紙や封印された荷物は検査に対して十分に保護されなければならないとしつつ、郵便物の外形や重量など、仲介者が保有する情報については例外であると判示した[58]。このときは、郵便物を開封するという物理的な「侵入」を伴わずに得られる情報であることが重視されたが、電子メールへの類推の可能性も指摘されている[59]。

通信内容と外形的情報の区別を電気通信に適用したのは、一九七九年のスミス（Smith）判決[60]である。上告申立人（被疑者）宅からの電話発信の状況を調べるため、捜査機関が電話会社にペン・レジスター（pen register ＝番号のダイヤル時に電話機から発せられる電子信号を記録する機器）を装備させたという事案で、合衆国最高裁は、「通信の内容を把握するものではないため、ペン・レジスターはカッツ事件で使用された盗聴器とは大きく異なる[61]」と述べた上で、次の二点を理由に、電話の発信番号に関して「プライバシーの正当な期待（legitimate expectation of privacy）」は認められないとした。

すなわち、①ダイヤルされた番号を電話会社が把握していることを利用者が認識していること[62]、②申立人は電話を利用する際、電話会社に対して発信番号を任意に伝達しており、電話会社がその情報を警察に開示するリスクを負ったものとみられること[63]、である。②の点は、第三者に対して任意に開示した情報については修正四条の保護が及ばないとする「第三者の法理（third-party doctrine）」に関わるもので、この考え方は別の判例で既に示唆されていたが[64]、本判決がこれを確立したものと理解されている[65]。

通信は一般に、第三者である事業者等を仲介してやり取りされるものであるから、およそ全ての通信は、その内容も含めて、第三者に開示されたものとみなすことも可能である。しかし、学説の多くは、「第三者の法理」が通信内容に及ぶものではないという立場をとる[66]。

（2）制定法

連邦法も基本的には、通信内容とそれ以外を分けて、それぞれに異なるレベルの権利保護を与える構造を採用し

ている。

一九八六年に制定された連邦法「電気通信プライバシー法（Electronic Communications Privacy Act＝ＥＣＰＡ）」は、通信内容に関するプライバシーに厚い保護を与えている。ＥＣＰＡの第Ⅰ編にあたる「通信傍受法（Wiretap Act）」は、一九六八年の「犯罪防止および街頭安全に関する包括法（Omnibus Crime Control and Safe Streets Act）」により新設された合衆国法典第一八編二五一〇条以下を改正したもので、有線通信（wired）・会話（oral）・電気通信（electronic）の傍受（interception）等を禁止する[67]。傍受は、所定の犯罪類型に関して相当な理由があると裁判官が認め、傍受命令（wiretap order）を発した場合に許される[68]。

これに対して、ＥＣＰＡの第Ⅲ編により、「ペン・レジスターおよびトラップ／トレース機器（Pen Registers and Trap and Trace Devices）」と題する諸規定が三一二一条以下に新設された。これは当初、前掲スミス判決の影響を受けたもので、特定の電話機からダイヤルされた電話番号を記録するペン・レジスターと、かかってきた電話番号を記録するトラップ／トレース機器の使用について定めている。これらの機器の使用にあたっては、「取得が見込まれる情報が、進行中の犯罪捜査に関連している」旨の申立てにより、裁判所の命令が発せられることが必要だが[69]、要件が緩やかなため行政的（ministerial）な手続であるとされる[70]。その後、二〇〇一年の「愛国者法（Patriot Act）」は、機器の定義を変更することで、インターネット通信にも適用できるようにした。具体的には、「いかなる通信の内容（contents of any communication）」を除いて、「発信・経路・到達・送信に関する情報（dialing, routing, addressing, or signaling information）」を記録、解読、捕捉するものとしたのである[71]。

以上の規定が、リアルタイムで行われる通信の傍受に関わるものであるのに対して、ＥＣＰＡの第Ⅱ編にあたる「通信記録法（Stored Communications Act）」で新設された合衆国法典第一八編二七〇一条以下は、電気通信サー

ビス（electronic communication service）および遠隔情報処理サービス（remote computing service）の提供者が保有する通信について定める。二七〇三条は、電気通信サービスの提供者が保有する過去一八〇日以内の通信の内容をついて「相当な理由」に基づく令状をもってのみ開示を請求できると定める[72]一方で、過去一八〇日を超えるもの（遠隔情報処理サービスの提供者が保有する通信も含む）については、令状を取得しない場合にも、裁判所等の提出命令で足りるとしている[73]。提出命令の手続は、通信の外形情報（利用者の氏名等）を開示させる場合[74]にも用いられるもので、前掲ペン・レジスターに関するものと同等の要件（捜査中の事件との関連性）が課されている[75]。そのため、通信内容の開示に関して、相当な理由に基づく令状よりも緩やかな手続を定めた本条の規定が、修正四条に違反する可能性を指摘する見解もある[76]。また、この点が、後掲の連邦下級審判例（ウォーシャック・ケース）においても問題となった。

（3）情報通信をめぐる連邦判例

修正四条の保障と情報通信の関係について判断を示した合衆国最高裁判例は未だ存在しないが、二件の連邦下級審判例がこの分野のリーディング・ケースとされている。

まずは、二〇〇七年のフォレスター（Forrester）ケース[77]である。本件の事案は、捜査機関が、被告人とその共犯者が麻薬を製造している疑いがあるとして、裁判所のペン・レジスター命令に基づいて、共犯者宅におけるインターネット通信を提供するＩＳＰにミラー・ポートを導入させ、共犯者が送受信した電子メールの宛先、アクセスしたウェブサイトのＩＰアドレス、データ送受信の総量に関する情報を取得したというものである[78]。第九巡回控訴

裁判所は、電話の発信番号を調べる本来の意味の「ペン・レジスター」の合憲性を認めた前掲スミス判決を引用しながら次のように判示して、本件捜査が修正四条に違反するものではないとした。

「電子メールとインターネットの利用者は、メッセージの宛先／差出人アドレスあるいは訪問したウェブサイトのＩＰアドレスについて、プライバシーの合理的期待を有しない。なぜならば、これらのメッセージの送信およびＩＰアドレスは、ＩＳＰその他の第三者の設備を通じて行われることを利用者らは当然認識しているからである。インターネットと電話それぞれによる通信は、第三者に対して情報を任意に提供することを利用者に要求するものである。[79]」

「宛先／差出人アドレスとＩＰアドレスは、送達情報（addressing information）を構成するものであり、その基礎にある通信内容を電話番号以上に暴露するものではない。ある者がダイヤルした電話番号を政府が知るとき、その番号が対応する人または組織を確定することができるかもしれないが、実際の会話で何が話されたかは知り得ない。同様に、電子メールの宛先／差出人アドレスまたは訪問先ウェブサイトのＩＰアドレスを政府が取得するとき、メッセージの内容や、その者が閲覧した当該ウェブサイト内の特定のページを把握することはできない。」

これに対して、ウォーシャック（Warshak）ケースにおいて、第六巡回控訴裁判所は、電子メールの中身が修正四条により保護されることを認めた。本件は、通信記録法の規定（前掲二七〇三条）により発せられた提出命令に基づき、郵便・通信詐欺等の嫌疑がかけられた被告人が送受信した二万七千通を超える電子メールの内容をＩＳＰから取得したという事案である。提出命令には、ＩＳＰが本件捜査の存在を被告人に知らせることを禁止するとと

もに、政府から被告人に対して行うべき通知も九〇日間遅らせる旨の条件が付されていたところ、本件捜査の存在を知った被告人が差止命令による救済を申し立てた。申立てを審理した第六巡回控訴裁判所は、二〇〇七年の判決[80]の中で、電子メールの内容について被告人にはプライバシーの合理的期待が認められるとした上で、たとえ通信記録法の規定に基づき提出命令によるとしても、事前の通知なしには許されない旨の判断を示したが、この判決は取り消された。しかし、再審理が行われた二〇一〇年の判決[81]で、改めて次のように判示したのである。

「電子メールが手紙または電話と類似すると考えるならば、修正四条と無関係に、政府職員が商業ＩＳＰに対して、電子メールの内容を引き渡すよう強制できないことは明らかである。ＩＳＰは電子メールによる通信を可能にする媒介者である。電子メールは、意図された受け手に到達するためにはＩＳＰのサーバーを通過しなければならない。従って、ＩＳＰは郵便局または電話会社と機能的には同等である。既に論じたとおり、警察が手紙を奪うために郵便局を襲うことは許されず、同様に、電話の会話を秘密裡に記録するために電話網を用いることは禁止されている――少なくとも、令状無くしては。政府職員が加入者の電子メールの内容を引き渡すようＩＳＰに対して強制するならば、当該職員はそれをもって、一部の例外を除き令状要件の遵守が求められる修正四条の捜索を行ったとみるべきことは、当然であるというほかない[82]。」

「政府は、相当な理由に基づく令状をまず取得することなしに、商業ＩＳＰに対して、加入者の電子メールの内容を引き渡すよう強制することはできない。従って、政府職員が被告人の電子メールの内容を入手したとき、令状を取得していないため、修正四条に違反したのである。さらに、このような電子メールを政府が令状無くして取得することを通信記録法が許容しているという限度において、通信記録法は違憲である[83]。」

3　近時の議論状況

（1）区別論に対する批判

現行の連邦法および連邦判例が、通信の内容とそれ以外の外形情報を区別し、前者のみに「プライバシーの合理的期待」を認めて修正四条による保護の対象にするという枠組みを採用していることは、ここまで見てきたとおりである。しかし、このような区別論に対しては批判が向けられている(84)。

批判の第一は、通信内容と外形情報が果たして明確に区別できるのかという疑問である。すなわち、通信の外形からその内容をある程度推知することが可能な場合があると指摘される。例えば、入学試験の合否通知が郵送されるとき、封筒の大きさで合格／不合格が予想できてしまうような場合である(85)。また、アクセスしたウェブサイトのＩＰアドレス（ＵＲＬ）は外形情報である一方で、どのような内容を閲覧したかも示唆するため、両者の区別が曖昧になるというのである(86)。

第二は、外形情報といえども通信内容と同等の保護を与えられるべきであるという異論である。両者の区別が困難であるという第一の批判と相まって、外形情報にも「プライバシーの合理的期待」が認められるべきであるとする(87)。このような指摘は従来からなされており、電話の発信番号を探知するペン・レジスターに関する前掲スミス判決に付されたステュワート裁判官（カッツ判決の法廷意見を執筆）の反対意見は、「［電話番号は］個人を識別し電話をかけた場所を容易に割り出すことができるため、個人の生活の奥にある細部を明らかにしてしまう」と論

じる。[88]

通信の外形情報が修正四条により保護されないという前提は、スミス判決が「第三者の法理」を用いて形成したものである。現在に至るまで、「第三者の法理」は、連邦法や連邦判例において、通信の外形情報にもなお妥当するものとされてきたが、とりわけインターネット通信に関しては、同法理の適用可能性を疑問視する見解がある。[89]

(2) モザイク理論

右のような主張の追い風になっているのが、いわゆる「モザイク理論（mosaic theory）」に理解を示しつつあるといわれる合衆国最高裁の近年の動向である。モザイク理論とは、プライバシーの観点からは取るに足りない個々の情報も、継続的な収集により集積されれば、保護されるべき個人情報を形成するという理論であり[90]、プライバシーをめぐる修正四条の議論において、現在「台風の目」ともいえるものである。「ビッグ・データ」の時代に適合し、また、通信の外形情報を保護に値するプライバシー情報に昇華させる途を開くものとされる。[91]

ジョーンズ・ケースを審理したDC巡回控訴裁判所は、二〇一〇年、共同被告人の名を冠したメイナード（Maynard）判決[92]で、このモザイク理論を採用した。まず、裁判所は、「プライバシーの期待が合理的か否かは、その期待が、公衆に晒された（exposed to the public）情報に関連するものかどうかに大きくかかってくる[93]」という前提を述べたで、一ヶ月以上にわたって他の者が観察し続けることは不可能であるから、被告人の移動の全過程が実際に（actually）公衆に晒されたとはいえないとした[94]。また、被告人の移動の全過程が擬制的にも（constructively）公衆に晒されたものとはいえず、GPS追跡装置を二八日間にわたり使用した結果、「他の誰かに知られているとと

は予想もしない、被告人の生活の細部にわたる光景[95]」が明かされたとして、本件捜査は修正四条に違反すると結論づけるにあたり、次のように指摘する。

「長期間にわたる監視は、人が繰り返し行うことや行わないこと、それを誰と行うかなど、短期間の監視によっては明かされない種類の情報を明らかにすることができる。こうした情報は、個人の行動を個別に観察する場合に比べて、ある者についてより多くのことを暴露することができる。教会、体育館、バー、競馬場への繰り返しの訪問は、それらの場所を一ヶ月以上にわたり訪問しないことと同様に、ただ一回の訪問の事実からは分からない実態を表す[96]。」

前掲ジョーンズ判決に付されたソトマイヨール（Sotomayor）裁判官の同意意見は、GPS追跡装置の取付けが車両に対する物理的侵入に該当するとした法廷意見への支持を表明する一方で、次のように、GPS追跡装置の使用自体が「プライバシーの合理的期待」を侵害する可能性に言及する[97]。

「GPSによる監視は、家族・政治・職業・宗教・性にかかる交際関係の詳細を反映する形で、個人の公共空間における行動の精密かつ包括的な記録を作り出すものである。政府は、将来的に何年にもわたって、こうした記録を保管し情報源として有効利用することができる。」

「政府が監視しているかもしれないという警戒心は、集団および表現の自由を萎縮させる。」

「私は、個人の公共空間における行動の総和に、プライバシーに関する合理的な社会の期待が存在するかを検討

する場合には、GPS監視のこのような特性を考慮する。私は、個人の政治的・宗教的信条、性的習慣等を政府が事実上随意に把握できるような形で、その行動が記録され集積されることを人々が正しく予期するか否かを問う。」

情報の集積が個人の行動の全体像を浮き彫りにするという旨の指摘は、モザイク理論に明らかに影響を受けたものとみられる[98]。右の言及を前提として、さらに、ソトマイヨール裁判官は「第三者の法理」を批判する。「個人が第三者に任意に開示した情報にはプライバシーの合理的期待がないとする前提を再検討する必要があるかもしれない。このアプローチは、日常的なタスクをこなす過程で人々が自身の情報を第三者に対して開示することになるデジタル時代には不適合である[99]。」

続いて、アリート（Alito）裁判官が執筆した同意意見も、モザイク理論に親和的な立場をとる。アリート裁判官は、法廷意見を厳しく批判した後に、ビーパーによる追跡が捜索にあたらないとしたノッツ（Knotts）判決[100]を引用し、同判決が短期間の監視であったのに対して、本件のような長期間にわたる監視は別問題であるとする[101]。

「大半の犯罪の捜査において、長期間のGPS監視は、プライバシーへの期待を侵害する。それらの犯罪に関しては、捜査機関等が個人の車両の移動の全てを非常に長期間にわたって秘密裡に監視し記録しないこと――そして現実には不可能であること――が、社会の予期するところだからである。」

ジョーンズ判決は、法廷意見よりもこれら二つの同意意見の方が注目に値するとまでいわれる。しかし、未だ合衆国最高裁の法廷意見として提示されたわけではないこのモザイク理論には、各捜査行為を別個に分析してきた従

来の方法や制定法との整合性や基準の明確性の観点から、有力な批判が向けられている[102]。

モザイク理論に対する合衆国最高裁のその後の立ち位置は、必ずしも明らかではない。関連問題について判断した二〇一四年のライリー（Riley）判決[103]が特に示唆しなかったからである。本件の事案は、逮捕に伴う無令状捜索により携帯電話内の記録を調べたというもので、被告人Aについては、携帯電話内に保存されていた写真から、銃撃事件への関与が明らかになった。被告人Bについては、「自宅（"my house"）」と表示された携帯電話の通話履歴からBの自宅を特定し、その場所を令状により捜索した[104]。ロバーツ（Roberts）長官の法廷意見は、逮捕者への危害または証拠の破壊を防止する目的において逮捕時の捜索が正当化されるというチャイメル（Chimel）判決[105]の基準等を満たさないため、本件捜索は修正四条に違反するとした。

右の結論に至る過程で、法廷意見が、通信内容／外形情報の区別論に立ち入ることはなかった。政府側が、通話履歴の捜索はスミス判決により正当化される旨を主張したのに対して、ペン・レジスターの使用が修正四条の捜索に該当しないとした同判決と、携帯電話の検査が捜索に該当することに争いがない本件とは異なるとして、この主張を退けたからである[106]。また、「本件が、他の状況において、集積されたデジタル情報の収集または検査が捜索に該当するか否かの問題に影響を与えることはない」とも述べて、モザイク理論との関連を否定している[107]。

また、下級審判例だが、二〇一二年のスキナー（Skinner）ケース[108]では、携帯電話から発せられる位置情報のデータを裁判所の命令に基づき電話会社から取得した事案で、同年のジョーンズ判決よりも後に下された第六巡回控訴裁判所の判決は、携帯電話の使用者が位置情報を任意に開示しており、さらに、位置情報に基づく追跡は尾行と異なるところがないとして、修正四条違反の主張を退けている[109]。

(19) 堀田周吾「任意性の相当性判断に関する一考察」首法四七巻二号（二〇〇六年）一二八頁以下。
(20) Boyd v. United States, 116 U.S. 616 (1886).
(21) *Id*. at 623.
(22) Entick v. Carrington, 95 Eng. Rep. 807 (1765).
(23) *Boyd*, at 630.
(24) *Boyd*, at 623.
(25) Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 Wake Forest L. Rev. 307 (1998) at 314-15.
(26) Clancy, *supra* note 25, at 314-19.
(27) Gouled v. United States, 255 U.S. 298 (1921) は´
(28) Olmstead v. United States, 277 U.S. 438 (1928).
(29) Clancy, *supra* note 25, at 312.
(30) *Olmstead*, at 456-57.
(31) *Olmstead*, at 465.
(32) *Olmstead*, at 466.
(33) *E.g.*, Silverman v. United States, 365 U.S. 505 (1961)［暖房ダクトに盗聴器を取り付けた行為が捜索にあたるとした事例］; Goldman v United States, 316 U.S. 129 (1942)［壁に取り付けた盗聴器で隣室の会話を聴取した行為が捜索にあたらないとした事例］; United States v Lee, 274 U.S. 559 (1927)［沿岸警備隊の探照灯の使用が捜索にあたらないとした事例］.
(34) 「侵入法理（trespass doctrine）」の呼称を用いる文献も多い。
(35) Morgan Cloud, *The Fourth Amendment During the Lochner Era: Privacy, Property and Liberty in Constitutional Theory*, 48 Stan. L. Rev. 555, 611 (1996).
(36) 詳細に検討した近年の国内文献として´宮下紘「ルイス・ブランスのプライバシー権―三四歳と七一歳のブランダイスをつなぐ言葉」駿河台二六巻一号（二〇一二年）七一頁以下。
(37) Katz v. United States, 389 U.S. 347 (1967).
(38) Warden v. Hayden, 387 U.S. 294 (1967).
(39) *Hayden*, at 300-301.

(40) *Hayden,* at 304.
(41) *Katz,* at 351.
(42) *Katz,* at 350.
(43) *Katz,* at 351.
(44) *Katz,* at 361 (Harlan, J., concurring).
(45) United States v. Jones, 132 S.Ct. 945 (2012).
(46) *Id.* at 948.
(47) United States v. Jones, 451 F.Supp.2d 71, 88 (D.D.C. 2006).
(48) *See*, United States v. Jones, 132 S.Ct. 945, 948-49 (2012).
(49) *Jones*, at 949.
(50) *Jones*, at 950.
(51) *E.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001).
(52) *Jones,* at 952.
(53) *Jones,* at 955 (Sotomayor, J., concurring).
(54) *Jones,* at 953.
(55) Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. Rev. 607, 611 (2003) は "envelope information" という表現を用いる。
(56) *See generally*, 2 Lafave Et Al., Criminal Procedure §4.4(b)-(d) (3d ed. 2007); Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 Santa Clara L. Rev. 821, 823-29 (2014); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005 (2010); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105 (2009).
(57) *Ex parte* Jackson, 96 U.S. 727 (1877).
(58) *Id.* at 733.
(59) Kerr, *supra* note 56, at 1022-23.
(60) Smith v. Maryland, 442 U.S. 735 (1979).
(61) *Id.* at 741.

(62) *Id.* at 742.
(63) *Id.* at 744.
(64) United States v. Miller, 425 U.S. 435, 442-44 (1976).
(65) *See generally,* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 569-70 (2009).
(66) *E.g.*, Kerr, *supra* note 56, at 1038.
(67) 18 U.S.C.A. §2511.
(68) 18 U.S.C.A. §2518.
(69) 18 U.S.C.A. §3122.
(70) 2 LAFAVE ET AL., CRIMINAL PROCEDURE §4.7(b)(3d ed. 2007).
(71) 18 U.S.C.A. §3127(3)-(4).
(72) 18 U.S.C.A. §2703(a).
(73) 18 U.S.C.A. §2703(b).
(74) 18 U.S.C.A. §2703(c).
(75) 18 U.S.C.A. §2703(d).
(76) Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 190 (2014); Kerr, *supra* note 56, 1043-44.
(77) United States v. Forrester, 495 F.3d 1041 (9th Cir. 2007).
(78) *Id.* at 1044.
(79) *Id.* at 1049.
(80) Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated on rehearing en banc, 532 F.3d 521 (6th Cir. 2008).
(81) United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).
(82) *Id.* at 286.
(83) *Id.* at 288.
(84) *E.g.,* Brad Turner, *When Big Data Meets Big Brother: Why Courts Should Apply United States v. Jones to Protect People's Data*, 16 N.C. J. L. & TECH. 377, 398-401 (2015); Conley, *supra* note 56, at 828-35; Daniel J. Solove, *Reconstructiong Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1286-89 (2004).

(85) Conley, *supra* note 56, at 831; Solove, *supra* note 84, at 1287.
(86) Conley, *supra* note 56, at 831; Solove, *supra* note 84, at 1287.
(87) Conley, *supra* note 56, at 831. *See also*, Kerr, *supra* note 56, at 1037.
(88) Smith v. Maryland, 442 U.S. 735, 748 (1979) (Stewart, J., dissenting).
(89) Serafino, *supra* note 76, at 165-70.
(90) *See generally*, David Gray et al., *Fighting Cybercrime After United States v. Jones*, 103 J. Crim. L. & Criminology 745 (2013).
(91) *See generally*, Monu Bedi, *Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. Rev. 1809, 1857-65 (2014); Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix-Doctrine to Follow*, 14 N.C. J. L. & Tech. 489 (2013); Christopher Slobogin, *Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 Duke J. Const. L. & Pub. Pol'y 1 (2012).
(92) United States v. Maynard, 615 F.3d 544 (2010).
(93) *Id.* at 558.
(94) *Id.* at 560.
(95) *Id.* at 563.
(96) *Id.* at 562.
(97) United States v. Jones, 132 S.Ct. 945, 955-56 (2012) (Sotomayor, J., concurring) .
(98) Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 Mich. L. Rev. 311, 328 (2012).
(99) *Jones,* at 957 (Sotomayor, J., concurring).
(100) United States v. Knotts, 460 U.S. 276 (1983).
(101) *Jones,* at 964 (Alito, J., concurring).
(102) Kerr, *supra* note 98.
(103) Riley v. California, 134 S. Ct. 2473 (2014).
(104) *Id*. at 2480-82.
(105) Chimel v. California, 395 U.S. 752 (1969).
(106) *Riley,* at 2492-93.
(107) *Riley,* at 2489 n.1.

（108） United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).
（109） *Id.* at 777-78.

三　結びにかえて

本稿では、情報通信にかかるプライバシーについて、アメリカ合衆国の近時の状況を分析した。人の所在情報と、通信にかかる情報とは、これを把握するための手段が異なるため、ＧＰＳによる追跡が修正四条に違反するとしたジョーンズ判決の法廷意見は、同判決の射程が情報通信には及ばないことを明らかにしている。他方、公共空間における人の所在は、外部から認識・把握することが可能であるという意味で、通信における電話番号やＩＰアドレス等と質的には共通する部分を有する。

従来、通信の内容と、電話番号やＩＰアドレス等の「外形情報」とが区別され、後者におけるプライバシーの要保護性は低いとされてきたが、ジョーンズ判決の同意意見が提起したように、プライバシーの観点からはとるに足りない個々の情報が集積されることによって新たな問題状況が生じるのだとすれば、通信の外形情報をめぐるプライバシー保護の必要性が今後再評価される可能性はある。一判決の同意意見を過大評価しないよう慎重であるべきだが、わが国刑訴法の母法国の動向は、こちらの議論にも少なからず影響を与えることが見込まれる。

わが国に目を向けると、刑訴法一九七条三項に基づく通信履歴の保全要請は、かかる情報を捜査機関が掌握する前段階の措置に過ぎないことから、通信の当事者との関係では問題を生じないが[110]、このような措置が可能であること自体、通信履歴の要保護性が低いとの評価に基づくものだともいえる。また、同二二二条の二における「電気

通信の傍受」は通信内容の傍受を意味するとして、電話番号や通信履歴等の外形情報の傍受は、厳格な手続による通信傍受令状ではなく、検証令状によるものとされる(111)。

このような区別論に対しては、通信履歴の保護を軽視するとの批判が向けられるが、通信内容を特に重要な保護領域と定め、とりわけ慎重な対応を要請することにつながる側面もあったのではないか。情報通信にかかるプライバシーをめぐる議論は新しい局面を迎えつつあるが、そこで両者の違いを相対化して「垣根」を取り除くとしても、深刻化するサイバー犯罪に対応するために事後追跡可能性を確保することの重要性を認識しつつ、プライバシー保護と捜査の実効性との適切なバランスを図らなければならない。

(110) 酒巻匡「サイバー犯罪条約の手続規定について」法とコンピュータ二一号（二〇〇三年）六〇頁、長沼範良「ハイテク犯罪と刑事手続法の整備」ジュリ一二五七号（二〇〇三年）二八頁、池田公博「電磁的記録を含む証拠の収集・保全に向けた手続の整備」ジュリ一四三一号（二〇一一年）八四頁参照。

(111) 電話番号等の逆探知は検証許可状によるとの理解を示すものとして、池田弥生「携帯電話の位置探索のための令状請求」判タ一〇九七号（二〇〇二年）二七頁以下、河上和雄ほか編『大コンメンタール刑事訴訟法［第二版］第四巻』（二〇一二年）六〇一頁［辻裕教］。

※前田雅英先生のサイバー犯罪に関する業績は多数ある。私自身、先生の下で勉強させていただいた東京都立大学の学部・大学院時代から、情報の問題には特に関心を持っており、その後、先生と共同執筆させていただく機会にも恵まれた（「個人識別情報の刑事的保護――『ID犯罪』の現状――」法律のひろば六一巻一〇号）。大変拙いものではあるが、先生と縁の深いテーマで本稿を執筆することで、先生からこれまで賜ったご学恩に感謝するとともに、今後の末永いご指導をお願いする次第である。